BTA

BUSINESS TRANSFORMATION AGENCY

DoD IT Business Systems
Investment Review Process

Investment Review Board Concept of Operations

July 12, 2006

Table of Contents

1.0 Introduction

The Department of Defense (DoD) is perhaps the largest and most complex organization in the world. Viewed as a business, it manages a budget that is more than twice that of the world's largest corporation, it employs more people than the populations of a third of the world's countries, it provides medical care for as many patients as the nation's largest health management organization, and it warehouses and manages five hundred times the number of inventory items as the world's largest commercial retail operation.

The sheer size of the Department, and particularly the complexity of its business operations, reflects the magnitude of its mission and the broad responsibilities it has for maintaining national security. This mission, however, also demands that the Department be as nimble, adaptive, flexible, and accountable as any organization in the world. Reconciling the apparent contradiction between size and flexibility – between complexity and adaptability – is the challenge of defense business transformation.

> *"Just as the U.S. forces operate jointly, so too must horizontal integration become an organizing principle for the Department's investment and enterprise-wide functions."*
>
> -- Quadrennial Defense Review Report (February 6, 2006)

The Department's IT business systems investment review process (referred to henceforth as the *IRB Process*) provides a framework for effective investment decision-making, enabling the Department's senior leadership to guide investments to maximize the impact to the warfighter. Led by the Deputy Secretary of Defense (DEPSECDEF), who chairs the Defense Business Systems Management Committee (DBSMC), with direct participation of the top leadership of each DoD Component, the Department is working to develop and implement integrated, cross-DoD business functions and capabilities. The process is guided by the Business Enterprise Architecture (BEA) and the Enterprise Transition Plan (ETP), which, along with associated Component architectures and transition plans, provide an integrated view of DoD business functions and a roadmap to deliver more robust business capabilities.

This Investment Review Process Overview and Concept of Operations for Investment Review Boards (referred to henceforth as the *IRB CONOPS*) is being updated to include additional guidance related to the Annual Review process and other policy refinements that will provide improved support to the DBSMC in effectively managing funding of business systems modernizations. Additionally, it will ensure compliance in meeting the requirements of the Ronald W. Reagan National Defense Authorization Act of Fiscal Year 2005 (referred to henceforth as the *FY 2005 NDAA*) (Title 10 U.S.C. section 2222).

2.0 Purpose

The IRB CONOPS integrates the policies, specifies responsibilities, and identifies the processes to establish and operate IRBs for the purpose of certifying business system modernizations in excess of $1 million over the system modernization's lifecycle. Additionally, it elaborates on applicable regulations, defines governance, roles and responsibilities, processes and controls for DoD Components in conducting annual reviews of all business system investments. The IRB CONOPS will be followed by the DBSMC, Principal Special Assistants, IRBs, Component Chief Information Officers (CIOs) and staffs who have responsibility for business systems and business system investments review processes as required by the FY 2005 NDAA.

This document replaces *the IRB CONOPS* dated May 17, 2005 and released on June 2, 2005. It is supplemented by the *Investment Certification and Annual Review Process User Guidance* (referred to henceforth as the *IRB Guidance*) updated concurrent with this document and the *Business Enterprise Architecture (BEA) Compliance Guidance* (referred to henceforth as the *BEA Compliance Guidance)*, dated April 10, 2006.

Upon reading this IRB CONOPS and all related guidance, PMs, Component CIOs, IRB Chairs and members as well as other stakeholders should understand the following:

- Why IRBs were established
- Who must comply with and use these processes
- When an IRB review, certification or annual review is required
- What governance, roles, information requirements, and products are associated with the IRB review, certification and annual review processes
- How to prepare for an IRB review
- How an IRB functions
- How to use the IRB process

3.0 Scope

The IRB CONOPS contains policies to be followed by the Office of the Secretary of Defense (OSD) level IRBs. Additionally, it defines the information exchanges and touch points between these IRBs and the DoD Components. The IRB CONOPS does not prescribe Component business system investment processes and procedures. Given this, delineation of responsibilities within individual Components may vary from the model presented in this document due to Component-specific practices. Components are required to establish their own investment review processes to manage their business systems portfolio and transformation activities, and to ensure compliance with the FY 2005 NDAA. Component processes and procedures should be consistent with applicable laws, regulations and this IRB CONOPS.

Business system investments reviewed by the IRBs cover the full spectrum of functions and capabilities supported by DoD Business Mission Area. Inherent in these evaluations are tradeoffs between systems and priorities, the optimization of departmental capabilities and the rationalization of the overall systems inventory in order to deliver integrated, end-to-end business capabilities to the warfighter. In this manner, the IRB Process supplements and compliments the requirements of IT Portfolio Management. The IRB Process requires business systems to leverage the Defense Acquisition process and Joint Capabilities Integration Development System (JCIDS) requirements generation processes to meet certification requirements where appropriate. The specifics of how these processes interrelate, however, is beyond the scope of this IRB CONOPS.

4.0 Background

4.1 The IRB Review, PSA/CA Certification, and DBSMC Approval

The FY 2005 NDAA states that funds may not be obligated for a defense business system modernization that will have a total cost in excess of $1 million unless —

> *(1) the approval authority designated for the defense business system certifies to the Defense Business Systems Management Committee established by section 186 of this title that the business system modernization--*
> *(A) is in compliance with the enterprise architecture;*
> *(B) is necessary to achieve a critical national security capability or address a critical requirement in an area such as security or safety; or*
> *(C) is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such adverse effect; and*
> *(2) the certification by the approval authority is approved by the Defense Business Systems Management Committee. (Title 10 U.S.C. section 2222 (a))*

NOTE: Systems with total modernization expenditures below $l million do not require an IRB review, Certification Authority (CA) certification or DBSMC approval unless the system or the business processes which it supports has been designated as Principal Staff Assistant (PSA) Interest Program by the CA.

4.2 The Annual Review

Additionally, the FY 2005 NDAA requires:

> *Periodic review, but not less than annually, of every defense business system investment. (Title 10 U.S.C. section 2222 (g)(2)(B))*

NOTE: The annual review requirement applies to *all* DoD business systems, not just those with current development/modernization efforts

4.3 Definitions as stated in the FY 2005 NDAA

The term *defense business system* means:

> *An information system, other than a national security system, operated by, for, or on behalf of the DoD including financial systems, mixed systems [financial and non-financial in one system], financial data feeder systems and information technology and information assurance infrastructure, used to support business activities, strategic planning and budgeting, installations and environment, and human resource management. (Title 10 U.S.C. section 2222 (j)(2))*

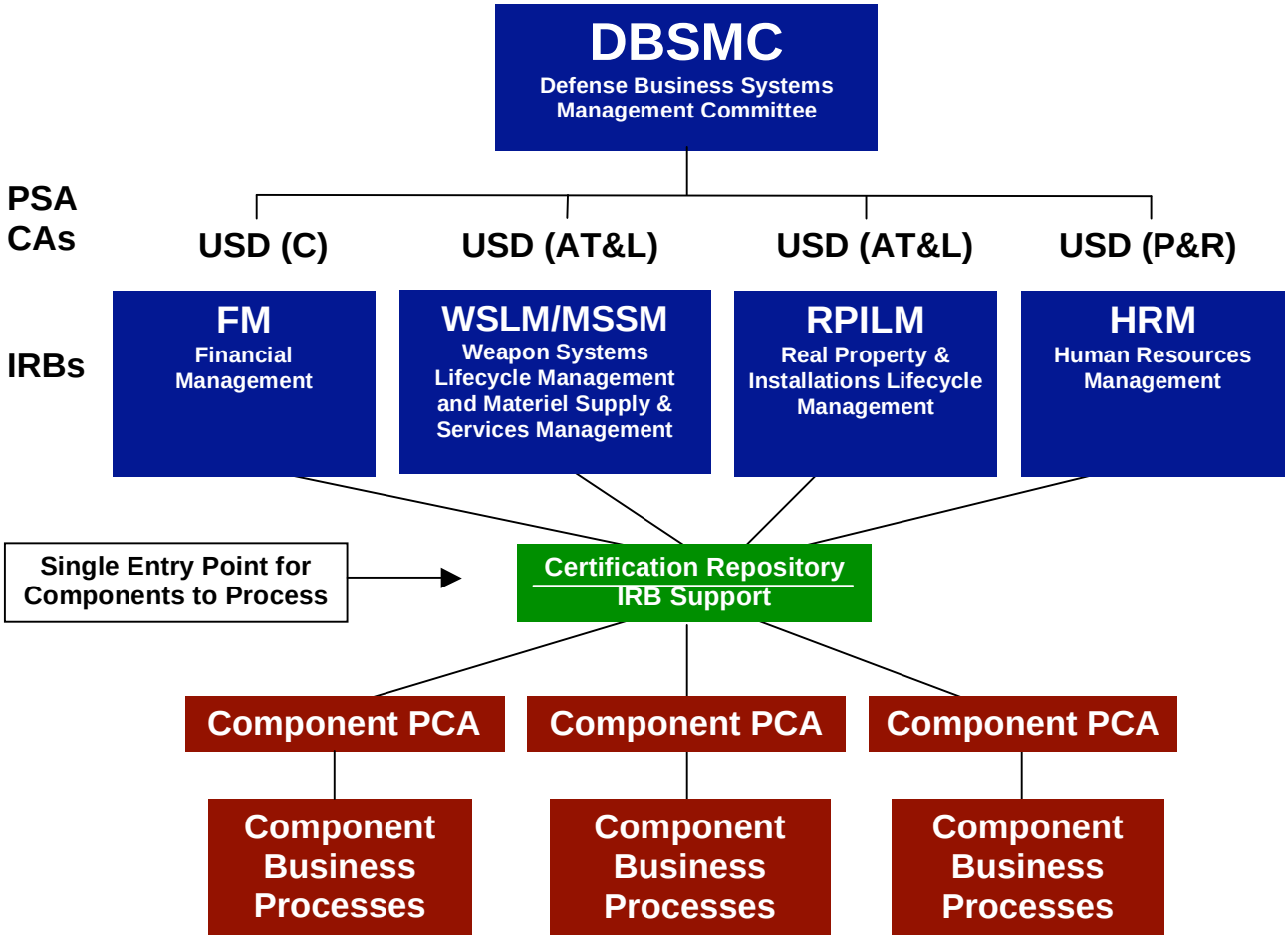
The term *business system modernization* means:

> *The acquisition or development of a new defense business system; or any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services). (Title 10 U.S.C. section 2222 (j)(3))*

5.0 Governance

The FY 2005 NDAA establishes an investment management governance organization that reports to the DEPSECDEF. This organization has responsibility for reviewing the planning, design, acquisition, development, deployment, operation, maintenance, modernization and project cost benefits and risks of defense business systems investments.

This governance structure and how it relates to DoD's Component organizations is illustrated below:



5.1 The Defense Business Systems Management Committee (DBSMC)

The DBSMC is chaired by the DEPSECDEF or the Vice Chair in his absence, and is responsible for approving business systems modernization investments in excess of $1 million, which have been certified by designated certification authorities. Its membership includes:

- Deputy Secretary of Defense (Chair)
- Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) (Vice Chair)
- Secretaries of the Military Departments and the heads of the Defense Agencies
- Under Secretary of Defense (Comptroller) (USD(C))

- Under Secretary of Defense for Personnel and Readiness (USD (P&R))
- Vice Chairman of the Joint Chiefs of Staff (JCS)
- Commander, U.S. Transportation Command (TRANSCOM)
- Commander, U.S. Joint Forces Command (JFCOM)
- Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DOD CIO)
- Director, Program Analysis and Evaluation (PA&E) (Advisory)

5.2 Certification Authority (CA)

The SECDEF delegated approval authority and accountability for defense business systems, and the systems that support them, to the following PSAs who, in addition to their other responsibilities within DoD, are designated certification authorities:

- USD(AT&L) – for acquisition, logistics, installation and environment activities
- USD(C) – for financial management activities
- USD(P&R) – for human resource management activities
- ASD(NII)/DoD CIO – for information technology infrastructure and information assurance activities in support of business systems
- DEPSECDEF - for DoD business activities not addressed above

5.3 Investment Review Boards (IRBs)

Per the FY 2005 NDAA and the DEPSECDEF's March 19, 2005 memorandum (see section 10.0, References), each of the CAs listed above is required to establish and charter an IRB to provide oversight of investment review processes for business systems supporting activities under their designated area of responsibility. To ensure consistency across all IRBs, standard operating procedures and guidelines are described in this IRB CONOPS and will be implemented by all IRBs. Exceptions must be approved by the DBSMC. IRBs are to include representatives from Combatant Commands (COCOMS), the Components, and the Joint Chiefs of Staff who will participate as appropriate based on the types of business activities and system modernizations being reviewed and certified.

5.4 Component Pre-Certification Authority (PCA)

Consistent with Title 40 U.S.C. section 11312, Components are expected to establish their own investment review governance structures and pre-certification authorities in support of their transformation initiatives. To ensure a smooth interface between the Component investment review organizations and the OSD level IRBs, each of the Components will designate one or more PCAs to act as the principal point(s) of contact. Their roles and responsibilities are defined below.

6.0 Roles & Responsibilities

6.1 Defense Business Systems Management Committee

The DBSMC will meet at least quarterly, although more frequent meetings may be called at the direction of the Chair. The role of the DBSMC is to:

- Recommend to SECDEF policies and procedures necessary to effectively integrate the requirements of the FY 2005 NDAA into all business activities and any transformation, reform, reorganization or process improvement initiatives undertaken within DoD
- Review and approve any major update of the defense business enterprise architecture under the FY 2005 NDAA, including evolving the architecture, and of defense business systems modernization plans
- Manage cross-domain integration consistent with an enterprise architecture

The DBSMC is responsible for coordinating defense business system modernization initiatives to maximize benefits and minimize costs and periodically report to SECDEF on the status of defense system modernization efforts. To meet these responsibilities, the DBSMC will coordinate activities required to:

- Establish strategic direction and plans for the Business Mission Area (BMA)
- Ensure the BMA efforts enable cross-Department, end-to-end interoperability
- Approve metrics and targets for tracking the business systems transformation progress
- Approve the BMA strategic plan, overall Business Enterprise Architecture and the Enterprise Transition Plan
- Approve certification by Approval Authorities (also known as Certification Authorities)
- Approve new enterprise solutions
- Comply with all public laws and annual reporting requirements and address all concerns from all oversight bodies
- Address IRB escalation issues
- Ensure processes, procedures, policies and investment review criteria are consistent across IRBs
- Ensure all IRBs provide consistent guidance to Component Pre-Certification Authorities

6.2 The Principal Staff Assistant (PSA) Certification Authorities (CAs)

The PSA CAs are assigned responsibility for the review, approval, and oversight of the planning, design, acquisition, deployment, operation, maintenance and modernization of the defense business systems assigned to them. PSAs are expected to set strategic objectives, establish policy, define enterprise level capabilities, and provide functional input into enterprise level architecture products, transition plans that support their core business mission. With respect to the IRB process, each PSA CA will:

- Establish, charter, designate members and stand up an IRB to review systems for which they are assigned responsibility
- Advocate DoD Enterprise Systems where appropriate
- Establish priorities and strategic direction for the business systems review process
- Review certification packages assigned to the business area and make certification decisions
- Identify specific systems or specific business processes as *PSA interest programs* and require review for systems that support those lines of business
- Ensure compliance this IRB CONOPS and the references listed therein
- Ensure timely coordination with other IRBs as required
- Report CA certification decisions to the appropriate IRB(s) and to the DBSMC
- Represent their core business mission on the DBSMC

6.3 Investment Review Boards

The IRB Chair will:

- Preside at IRB meetings
- Appoint additional members to the IRB as appropriate
- Ensure participation on other IRBs as required
- Adhere to the standard processes and procedures that apply to all IRBs
- Ensure alignment with PSA priorities
- Lead the establishment and implementation of specific criteria for business system certification and review
- Engage Component PCAs to accomplish required business system certification and annual reviews

The IRBs will:

- Review business systems and initiatives for compliance to the BEA
- Ensure review of every Tier 1-3 business system modernization investment at least annually
- Perform the appropriate level of review using a *Tiered Process* which links level of review to scope, complexity, cost, and risk
- Review and approve the enterprise criteria for that IRB
- Recommend to the IRB Chair and CA certification or non-certification based on certification criteria
- Recommend to the IRB Chair and CA approval for new enterprise solutions

6.4 IRB Support Staffs

IRB Support staffs will:

- Maintain IRB related documents in the designated global IRB document repository that contains all IRB related documents and serves as the official audit trail for the IRB certification and annual review processes
- Maintain IRB decisional related data in the DoD's official IT repository
- Assist the IRBs in executing their roles and responsibilities with Components
- Serve as the single point of contact for all Component questions regarding the IRB certification process and annual review processes

6.5 Component PCAs

Each Component is responsible for designating a PCA who is assigned accountability for the Component's business system investments. The Component may decide to designate a single PCA for all business systems or designate a PCA for each of its core business mission areas. However, in no case should there be more than one PCA per Component, per business mission area (IRB). Component PCAs will:

- Designate the office and person at the Component level responsible for system reviews and compliance with the FY 2005 NDAA. A copy of the designation letter for Component PCAs must be provided to the DBSMC Chair and IRB support staffs annually or whenever there is a change to the office or representative
- Establish the Component's own investment review processes and governance structure (consistent with Title 40 U.S.C. section 11312) to support Component transformation initiatives
- Ensure Component level investment review processes integrate with the IRB Guidance and BEA Compliance Guidance and accurately reflect the policies, procedures and governing principles outlined in this IRB CONOPS
- Identify those Component systems that require IRB certification
- Prepare, review, approve and upload all required IRB certification and annual review documentation to the IRB portal
- Participate in IRBs as designated members if appointed
- Assess and pre-certify architecture compliance of systems submitted for certification and review and approve all architecture compliance plans
- Verify that systems are recorded accurately in the Component and Enterprise transition plans as required.
- Validate information in the Department's global business systems inventory as being current, complete and accurate
- Ensure Component's budget office receives any changes to a system's development/modernization funding appropriation as a result of an investment review or annual review

6.6 Program Managers (PMs)

All PMs must understand that their systems are subject to IRB certification and annual reviews by multiple levels of authorities, including the Component PCA, the appropriate IRB, and the DBSMC. Specifically, PMs will:

- Ensure program information provided to the PCA is current, complete and accurate
- Verify that the IRB and the DBSMC, via the Component PCA, have completed system review, certification, and approval before obligating funds over $l million for modernization
- Ensure the business system complies with the BEA or has a documented plan (Compliance Plan) to achieve compliance
- Ensure the business system is included in the Component and/or Enterprise transition plans as appropriate

7.0 Investment Review Process

7.1 Identifying Systems for Certification

It is the Component's responsibility to:

- Identify business systems that require certification
- Prepare and validate information required for the certification process
- Upload certification documentation to the IRB portal in a timely fashion to ensure funds are not inappropriately obligated.

The IRBs assist the Components in identifying systems that require certification through analysis of the annual IT budget and other mechanisms. Ultimately, the CAs and IRBs determine what systems require certification and when those systems should submit their certification packages. A CA or IRB may require any system, regardless of the size of its development or modernization effort, to come in for certification by declaring the system a *PSA Interest Program*.

It is possible that a system may have multiple, non-related enhancements active simultaneously. In these situations, however, Components should discuss the program in question with the appropriate IRB. Ultimately, the decision as to whether these enhancements need to be aggregated into a single certification request or remain as separate modernizations each below $1 million, is left to the CAs and IRBs.

In situations where previously certified systems receive substantial end-of-year funding, it is strongly recommended that the system resubmit the certification package for the full amount of funding requested (both original and new funds). This consolidation of certified funding substantially simplifies oversight and eliminates any need for multiple annual reviews in following years. (NOTE: When this is done, previous certification conditions will be applied to the new certification except where there is substantiating evidence that specific conditions have been satisfied.)

7.2 Review Categorized by Tiers

All development/modernization efforts are assigned a *Tier* based on acquisition category and/or the size of the financial investment. The investment *Tiers* are defined as follows:

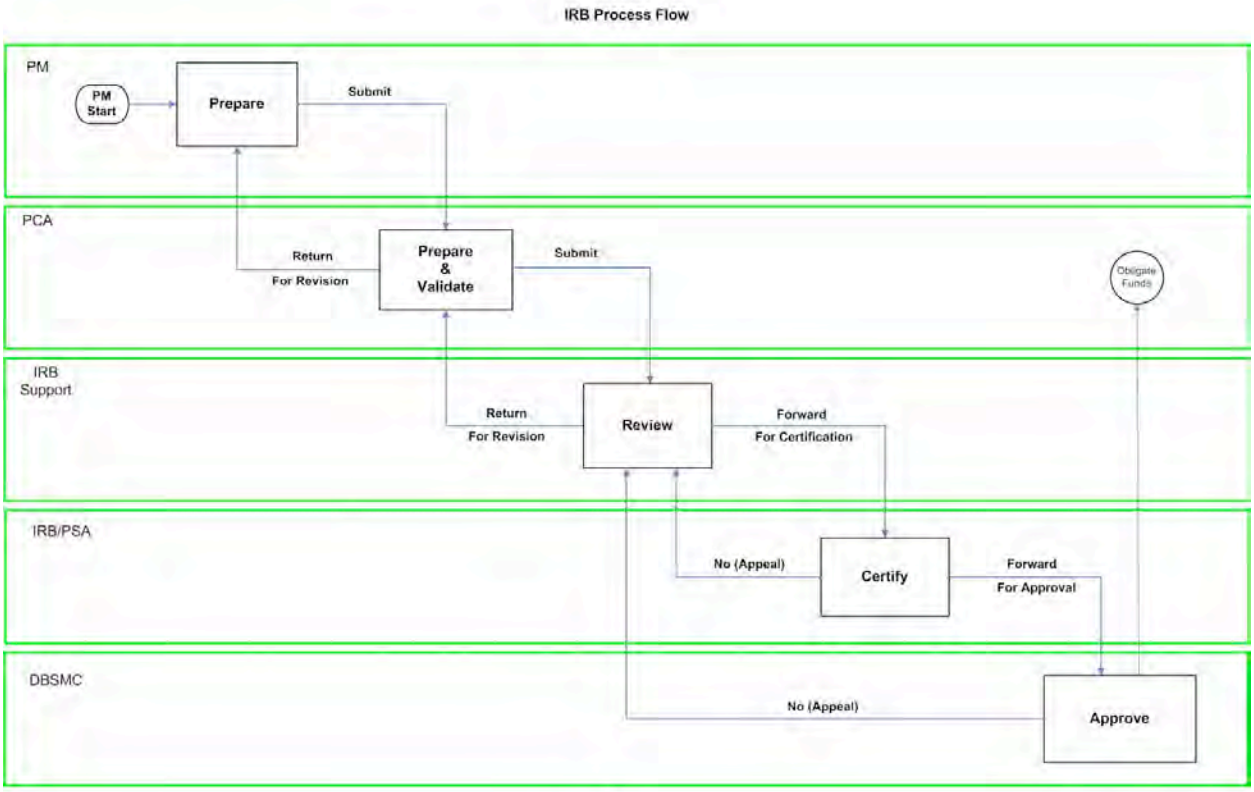
- Tier 1 – Includes all MAIS programs – ACAT 1A, ACAT 1AM, or ACAT 1D
- Tier 2 – Includes all non-MAIS program investments $10 million or above
- Tier 3 – Includes all non-MAIS program investments greater than $1 million and less than $10 million
- Tier 4 – Includes all non-MAIS program investments less than or equal to $1 million

All development/modernization efforts falling in Tiers 1, 2, and 3 require IRB review, CA certification and DBSMC approval. All Tier 4 development / modernization efforts are approved at the Component level, unless they have been deemed a *PSA Interest Program* by a CA or IRB, in which case IRB review is required.

All systems are required to maintain full, complete and accurate information in the Department's global business systems inventory. Component PCAs generate certification documentation (except the PCA Pre-certification Letter) largely as reports from this data. Tier 1 reviews may leverage the Defense Acquisition and JCIDS processes, which have their own documentation requirements, to meet their certifications requirements; thus, additional documentation related to these processes is typically required. For Tiers 2 and 3 there is essentially no difference, from a Component's perspective, in the core documentation required for IRB certifications. It should be expected, however, that the degree of scrutiny applied by the IRBs, including the amount of additional questions a program may be asked to prepare answers to, will vary in proportion to the size of the investment.

7.3 IRB Process Steps

The following discussion and diagram provide a high level view of the IRB process flow. It summarizes each participant's responsibility in the IRB process and highlights significant gating factors that enable the process to move forward. A more detailed view of the process is described in the IRB Guidance.



7.3.1 Program Manager (PM) Preparation

PMs are the primary subject matter experts for all information pertaining to systems they manage. As such, they serve as the focal point for maintaining all system data in the Department's global business systems inventory for the purpose of enabling system visibility, documenting compliance with a variety of internal and external policies and regulations, and, when necessary, for the IRB process. When a system is identified for review and modernization funds are requested, the PM should coordinate with the PCA to ensure all information required for certification is current and accurate.

7.3.2 PCA Preparation and Validation

PCAs are responsible for internal certification and review of systems modernization funding requests by PMs and for development and maintenance of the Component level business systems architecture and transition plan. PCAs are required to comply with investment review policies prescribed by the Component and by this CONOPS. For business systems modernizations that have been identified as requiring certification, the PCA is required to:

- Validate all system and certification information in the Department's global business systems inventory is current and accurate
- Validate that the system is compliant to the DoD Business Enterprise Architecture (BEA)
- Review and validate all documentation required for the IRB process which includes the PCA Pre-certification Assertion Letter, IRB Dashboard, an Economic Viability analysis and other documentation as described in detail in the IRB Guidance

- Post all required certification documentation on the IRB Portal, which serves as the authoritative audit trail for all investment certification and review activities

No Component system certification package will be considered by any IRB unless all required documentation is complete.

7.3.3 IRB Support Staff Review and Support

While the IRB Support Staff has no decision-making authority, it plays a vital role in coordinating activities between the Components (PCAs/PMs) and IRBs throughout the IRB Process. The IRB Support Staff supports the IRBs in identifying systems that require certification, scheduling systems on the IRB and DBSMC review calendars, facilitating and supporting IRB meetings and preparing issue papers, IRB minutes and other documentation.

To assist the Components, the IRB Support Staff serves as the single point of contact for all IRBs, reviews all certification package submissions for completeness and facilitates all cross-IRB coordination issues. The IRB Support Staff maintains metrics and develops strategies for process improvements and accountability. Throughout the process, the IRB Support Staff serves as a focal point for communication and issue resolution.

7.3.4 IRB Recommendation/CA Certification

IRBs review and recommend decisions on all requests for certification. IRBs evaluate systems based on a variety of criteria, to:

- Ensure business capabilities are delivered that support the warfighter
- Enable transformation by ensuring investments align with DoD strategic mission, goals and objectives and with BMA capabilities
- Ensure compliance with the DoD Business Enterprise Architecture and alignment to the ETP
- Exploit common processes and systems where feasible
- Ensure an appropriate level of review based on cost, scope, and complexity
- Comply with the legislation, regulations, policies and procedures outlined in this IRB CONOPS and other directives as appropriate

Evaluation may be achieved through paper coordination or by through direct face-to-face meetings. Face-to-face meetings are scheduled at the direction of the IRB Chair. The IRB Chair determines the format and structure for meetings and the level of participation from the Component PCA and other IRBs as appropriate. Programs that cross BMAs will invite representatives from all affected IRBs to participate in review activities. Actual participation is discretionary. Usually, the responsible Component PCA, and program personnel will be asked to attend. The type(s) of systems being reviewed will determine Component attendees. For example, a review of an inventory management system would most likely include the Defense Logistics Agency; a transportation system would most likely include representation from the US Transportation Command, etc.

For certifications that require coordination with other IRBs, the Lead IRB must ensure that all information is provided to all interested IRBs. The interested IRBs must participate in the review with the Lead IRB to avoid duplicative reviews of the same request.

The IRB Chair makes certification recommendations to the appropriate CA, who (assuming agreement) recommends approval of the certification via a memorandum to the Vice Chair of the DBSMC. IRB members, affected programs and Components are copied on the memo which is posted on the IRB Portal along with other IRB related documents.

Recommendations for certification approval are specific as to the amount of funding certified and the time period for which the certification is active. IRBs/CAs may also place conditions on certifications which Components and system owners are required to meet. Conditions are documented and tracked for compliance; the status will be reviewed by the IRB during a system's annual review.

In cases where certification is not recommended, issues preventing certification will be documented by the IRB, submitted to the affected program and Component PCA and a copy stored in the system's folder on the IRB

Portal. Once the issues have been addressed, Component PCA may resubmit the investment modernization to the IRB process.

7.3.5 DBSMC Approval

The DBSMC will be notified of all CA certification decisions. If no objections are raised, DBSMC members will approve CA recommendations, and the DBSMC approval recommendation will be forwarded to the DBSMC Chair (or designee) for signature. The date the approval memo is signed becomes the official approval date and will be recorded in the Department's global business systems inventory.

In cases where the DBSMC disapproves a certification, the IRB process will end and the Component PCA will be notified. Issues preventing certification approval will be documented as in the case of IRB disapproval. Component PCAs may resubmit the investment modernization to the IRB process once any outstanding issues are addressed as appropriate.

The DBSMC's Certification approval memo and meeting minutes will be posted to the IRB Portal. It is the Component PCA's responsibility to ensure that PMs are notified of all IRB and DBSMC decisions and action items. If the certification is approved, the PCA should ensure that his budget office is notified of the amount of funds and timeframe approved for the system modernization and any conditions attached.

7.4 Transfer of Systems between IRBs within a BMA and Between DoD Mission Areas

Transfer of primary responsibility for a business system from one IRB to another within the BMA will be based on the functions and capabilities of the system and the alignment to the PSA area of responsibility. Both PSAs must agree to the transfer and coordinate with the Component PCA. Once an agreement has been reached, the IRB that has assumed ownership of the system will provide written notification of this transfer to the Component PCA. Component PCAs are responsible for updating BMA/IRB assignment in both the Department's global business systems inventory and the IT budget database.

Transfer of primary responsibility for a system between Mission Areas (MAs) (Business, Warfighter, Enterprise Information Environment (EIE), Intelligence) will be based on the functions and capabilities of the system as it relates to the MAs in question. In situations where a system is being considered for transfer into or out of the BMA, both the BMA PSA and the equivalent representative from the targeted MA must agree to the transfer and provide written notification of this transfer to the Component PCA. Once a transfer has been approved, it is the responsibility of the Component PCA to update the Department's global business systems inventory and the IT budget database appropriately. In situations where transfer between mission areas is desired and no agreement can be reached between the appropriate MA leads, the final decision is adjudicated by the DoD CIO as directed in the DoD Portfolio Management Directive and Instruction.

A word of caution – many systems support multiple DoD Mission Areas and/or multiple functions within the Business Mission Area. Reassignment of a system into or out of the BMA or between BMA IRBs never eliminates the requirement that all DoD systems must be compliant with the Business Enterprise Architecture.

8.0 Annual Review and Reporting Process

The FY 2005 NDAA requires *a periodic review, but not less than annually of every defense business system investment (*Title 10 U.S.C. section 2222 (g)(2)(B)). All DoD business systems must be reviewed at least annually.

Components are required to annually review *all* business systems, regardless of investment Tier, including systems for which there is no planned development or modernization spending. The FY 2005 NDAA does not prescribe any specific format for annual review; therefore, Components may structure these reviews in whatever way they deem most appropriate. It is anticipated that Components will incorporate the annual review requirement into their currently existing annual review activities such as portfolio management or annual budget preparation. At a minimum, as part of the annual reviews Components should make sure that systems are assessed against the DoD BEA, ensure systems are included in the Component or Enterprise Transition Plan, and that all required information regarding each system has been updated in the Department's global business systems inventory. Components are required to submit a letter to the IRBs on a semi-annual basis, on a schedule consistent with the Enterprise Transition Plan update cycle, listing all business systems that have been reviewed. These internal Component reviews, coupled with notification of these reviews to the CA / IRB, meet the FY 2005 NDAA annual review requirement.

In addition to annual reviews conducted at the Component level, the IRBs will conduct annual reviews of all development / modernization activities that have been certified and are currently in process. As described in detail in the IRB Guidance and BEA Compliance Guidance, these reviews will focus on:

- Continued compliance with the Business Enterprise Architecture (BEA)
- Program performance in terms of cost, milestone achievement and assessment of program risk against what was originally certified
- Progress towards meeting any conditions placed on program certifications by an IRBs or DBSMC

As such, the IRB Annual Review process is geared to highlighting issues related to delivery of capabilities as promised. The IRB Annual Review process is very similar to the IRB Certification process except that DBSMC action is not required. Like the IRB Certification process, the IRB Annual Review process will leverage information from the required documentation posted to the IRB Portal by the Component. Based on information reviewed, the IRBs may declare certification conditions closed or add new conditions as deemed appropriate. In cases where systems have significantly failed in achieving commitments made during IRB Certification, the IRBs may require recertification of the system in question. In these instances, IRBs will notify the DBSMC of this decision. IRB Annual review results are documented in the IRB meeting minutes which are posted to the IRB portal.

9.0 Documentation, Reports, Data Repository and Automated Tool

The following table summarizes the documents, reports, data repository inputs and tool updates requirements of various stakeholders and used in the investment review process.

System Review and Certification Documentation and Tools

Responsibility	Documents	System/Tool Updates
Component – Tiers 1-3 systems	• Prepare and submit required IRB certification package to include: Certification Dashboard, System Regulatory Compliance Report, and Economic Viability (EV) analysis prepared by Component or independent cost review authority (if DoD global business systems inventory's EV capability was not used) • Component Pre-Certification letter	• Update the DoD global business systems inventory with system information OR provide system information to the Component PCA to perform the Inventory update • Upload certification submission package to the IRB Portal
IRB and Support Staff	• Prepare certification CA memos and summary reports • Document IRB proceedings and voting results	• Update the DoD global business systems inventory with IRB and DBSMC results • Update the DoD global business systems inventory with certification and approval results and dates • Post IRB related correspondence, minutes, briefings to the IRB portal
PSA CA	• Sign CA Certification letter for transmittal to the DBSMC	
DBSMC	• Review and approve Annual Reports to Congress • Sign and issue DBSMC Certification Approval memo • Prepare and approve minutes of DBSMC meetings	

IRB Annual Review Documentation and Tools

Responsibility	Documents	System/Tool Updates
Component – All systems	• Prepare annual review letter to IRB	
Component – Tiers 1-3 systems	• Prepare and submit required Annual Review package to include: Annual Review Dashboard and Component PCA Annual Review Assertion Letter	• Update the DoD global business systems inventory with system information OR provide system information to the Component PCA to perform the Inventory update • Submit Annual Review submission package to the IRB Portal
IRB and Support Staff	• Prepare Annual Review memos and summary reports for PSA CA	• Update the DoD global business systems inventory with Annual Review results
PSA CA	• Signed CA Certification letter for transmittal to the DBSMC including list of systems having completed Annual Review	

10.0 References

- Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375), Section 332 which enacted Title 10 U.S.C. section 2222
- Title 40 U.S.C. section 11312, *Capital Planning and Investment Control* (Public Law 107-217)
- DEPSECDEF Memo, 19 March 2005, *Delegation of Authority and Direction to Establish an Investment Review Process for Defense Business Systems*
- *Investment Certification and Annual Review Process User Guidance*, April 10, 2006 (http://www.dod.mil/dbt/tools_certification.html)
- *Business Enterprise Architecture (BEA) Compliance Guidance*, April 10, 2006 (http://www.dod.mil/dbt/tools_certification.html)

11.0 Key Definitions

Term	Definition
ACAT IA	Programs which are Major Automated Information Systems (MAIS) or programs designated by ASD (NII) to be ACAT IA. The Milestone Decision Authority is the DoD CIO.
ACAT IAM	Is a sub-category of ACAT IA and is a program for which the Milestone Decision Authority (MDA) is the DoD Chief Information Officer (CIO)
ACAT IAD	A MDA designated special interest program or a program that will require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than $365 million
Application	A software program that performs a specific function directly for a user and can be

Term	Definition
	executed without access to system control, monitoring or administrative privileges.
Business Capability	The ability to execute a specific course of action. It can be a single business enabler or a combination of business enablers (e.g. business processes, policies, people, tools or systems, information) that assists an organization in delivering value to its customer.
Business Enterprise Architecture	The Business Enterprise Architecture (BEA) is a blueprint to guide and constrain investments in DoD organization, operations, and systems as they relate to or impact business operations. It will provide the basis for the planning, development, and implementation of business management systems that comply with Federal mandates and requirements, and will produce accurate, reliable, timely, and compliant information for DoD staff. PSAs will define the level of specificity for their areas of responsibility.
Business System	An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (Title 10 U.S.C. section 2222 (j)(2)) In addition, the DODD 8500.1 further defines a system as a *set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.*
Business System Modernization Investment	The acquisition or development of a new defense business system; or any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services).
Capability	The ability to execute a specified course of action. It is defined by an operational user and expressed in broad terms in the format of an Initial Capabilities Document (ICD), or a Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities (DOTMLPF) change recommendation.
Component	DoD Components are defined to be the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, the DoD field activities, and all other organizational and operational entities within the DoD.
Computer Network	The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.
Core System	An existing system, a system in development, or a system beginning the acquisition process that is/will become the Department's solution for a given capability(ies), as designated by the PSA.
Department, the	The Department of Defense
DoD Enterprise Systems	Systems that have been identified to become the standard across the Department of Defense
DoD Enterprise Transition Plan	A plan describing: (A) The acquisition strategy for new systems that are expected to be needed to complete the defense business enterprise architecture. (B) A listing of the defense business systems as of December 2, 2002 (known as legacy systems), that will not be part of the objective defense business

Term	Definition
	enterprise architecture, together with the strategy for terminating those legacy systems that provides for reducing the use of those legacy systems in phases. (C) A listing of the legacy systems (referred to in subparagraph (B)) that will be a part of the objective defense business systems, together with a strategy for making the modifications to those systems that will be needed to ensure that such systems comply with the defense business enterprise architecture. Each of the strategies *[above]* shall include specific time-phased milestones, performance metrics, and a statement of the financial and non-financial resources needs.
Global Information Grid	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.
Information Assurance	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— • Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; • Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and • Availability, which means ensuring timely and reliable access to and use of information.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the an executive agency (DoD). For purposes of the preceding sentence, equipment is used by an executive agency (DoD) or f the equipment is used directly by the DoD or is used by a contractor under a contract with the executive agency (DoD) which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term *information technology* does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.
Information Technology (IT) Portfolio	A grouping of the IT capabilities, IT systems, IT services, and IT system support services (e.g. IT required to support and maintain systems), management, and related investments required to accomplish a specific functional goal. Decisions to make, modify, or terminate IT investments shall be based on the Global Information Grid (GIG) integrated architecture, mission area goals, risk tolerance levels, potential returns, outcome goals, and performance.
Information Technology (IT) System	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Any Acquisition Category (ACAT) system that meets these criteria, anything categorized as a National Security System (NSS) or a Mission Assurance Category (MAC) level is, by definition, considered to be an IT system. Other types of IT systems include:

Term	Definition
	DoD-wide, Joint systems • Federal System used by DoD or supported by DoD • DoD System used as a Federal System • Multi- System • Standard System • Major Command Standard System (Echelon 2 or equivalent for Navy and Marine Corps) • Below Major Command System (below Echelon 2 or equivalent for Navy and Marine Corps) (e.g., bridges, uniques used at a single site) • Data Stores/Data Warehouses • Enclaves - Portals (Enterprise) - Automated Information System (AIS) Application
Interim System	An existing system or system in development, as designated by the PSA, that supports the Department for a given capability during a limited period of time. An interim system may have the potential to become part of the core solution.
IRB Item of Interest	Any program, system, initiative, process or other business-related function an IRB wishes to address.
Legacy System	An existing system that is designated for closure when the capability is absorbed by an interim or core system or if the capability is no longer required.
Major Automated Information System (MAIS)	A MAIS is a Major Automated Information System (MAIS) program that is: 1) designated by the OSD(NII) as an MAIS; or 2) estimated to require program costs in any single year in excess of $32 million (FY 2000 constant dollars) or total program costs in excess of $126 million (FY 2000 constant dollars). MAIS do not include Information Technology (IT) that involves equipment that is an integral part of a weapons system or is an acquisition services program.
Modernization	All costs, of any type of funding, incurred to design, develop, implement/deploy and/or functionally enhance/technically upgrade an information technology system. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency and inter-agency services from other Federal agencies. Does not include sustainment costs. Sources, OMB A-11, A-130
National Security Systems (NSS)	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency the function, operation, or use of which— involves intelligence activities: • involves cryptologic activities related to national security; • involves command and control of military forces; • involves equipment that is an integral part of a weapon or weapons system; or • subject to Information Security in order to provide Confidentiality, is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Net-Centric Operations and Warfare (NCOW)	The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core

Term	Definition
Reference Model	services, Community of Interest services, and environment control services), and the enterprise management components. It is also describes a selected set of key standards that shall be needed as the NCOW capabilities of the GIG are realized.
Portal	Provide a single web *location* from which many services and communications systems are accessed. May also be the establishment of a single secure web access point from which applications and information may be distributed. To enable enterprise portal services there must be: Web services, a global directory service, and PKI.
Portfolio Management	The management of selected groupings of IT investments using integrated strategic planning integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investment strategies. The core activities associated with portfolio management are analysis, selection, control, and evaluation.
PSA/CA Interest Program	A program may be special interest based on one or more of the following factors: technological complexity; Congressional interest; a large commitment of resources; the program is critical to achievement of a capability or set of capabilities; or the program is a joint program. Exhibiting one or more of these characteristics, however, shall not automatically lead to a *special interest* designation.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions Department of Defense Architecture Framework (DODAF). **Sub-system:** A distinct element of a system that can stand alone outside of its system environment **Module:** A distinct element of a system that cannot stand alone outside of its system environment. **Family of Systems:** A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation. **System of Systems:** A set or arrangement of independent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

12.0 Acronyms

Acronym	Definition
ACAT	Acquisition Category
ASD (NII/CIO)	Assistant Secretary of Defense for Networks and Information Integration/DoD CIO
AT&L	Acquisition, Technology and Logistics
BEA	Business Enterprise Architecture
BMMP	Business Management Modernization Program (formerly Financial Management Modernization Program, now absorbed into the Business Transformation Agency
BTA	Business Transformation Agency
CA	Certification Authority
CBM	Core Business Mission
CIO	Chief Information Officer
COCOMS	Combatant Commanders
DBSMC	Defense Business Systems Management Committee
DEPSECDEF	Deputy Secretary of Defense
DoD	Department of Defense
EIE	Enterprise Information Environment
ETP	Enterprise Transition Plan
FM	Financial Management
FY	Fiscal Year
HRM	Human Resources Management
IRB	Investment Review Board
IT	Information Technology
JCIDS	Joint Capabilities Integration Development System
JCS	Joint Chiefs of Staff
JFCOM	U.S. Joint Forces Command
MAC	Mission Assurance Category
MAIS	Major Automated Information System
MSSM	Material Supply and Service Management
NDAA	National Defense Authorization Act
NII	Networks and Information Integration
NSS	National Security System
OSD	Office of the Secretary of Defense
PA&E	Program Analysis and Evaluation
PCA	Pre-Certification Authority
PSA	Principal Staff Assistant
WMA	Warfighting Mission Area